1998 Paper 8 Question 6

Advanced Algorithms

Suppose you are presented with a (large) integer N and are asked to find its complete factorisation. You are not told anything at all in advance about how many factors it will have, but you are instructed to use the Pollard Rho method as a probabilistic algorithm as the core of your code. Explain

(a) The overall structure of the code you would write, where it calls Pollard Rho and any other sub-algorithms you will use, and what their purpose is. [4 marks]

(b) What steps are taken in the Rho method and (informally) why it might be hoped that it will do what it is expected to. [6 marks]

(c) The extents and manners in which parts of your code rely on random numbers and the consequences of these turning out to be either especially fortunate or especially awkward. [5 marks]

(d) A coarse estimate of the total run-time for the factoriser in circumstances when the input number has exactly two large prime factors, and an equally crude estimate of the size that N would need to be before the factorisation process took a whole day of CPU time on a modern desktop workstation. You may suppose that around 10^{13} basic operations are available in that amount of time. [5 marks]